July 29, 2021

Office of Strategy, Policy and Plans
Department of Homeland Security (DHS)
245 Murray Lane, S.W.
Washington, D.C. 20528
Docket No. DHS-2020-0028

submitted via https://www.regulations.gov

Comment of the American Civil Liberties Union ("ACLU"), the Electronic Frontier Foundation ("EFF"), and the Electronic Privacy Information Center (EPIC)
RE: Minimum Standards for Driver's Licenses and Identification Cards Acceptable by Federal Agencies for Official Purposes; Mobile Driver's Licenses (Docket No. DHS-2020-0028)

A system of mobile or digital driver's license and/or identification documents (mDL), as contemplated by the Department of Homeland Security, implicates important privacy and free expression interests.[1] We have a number of concerns over such a system and whether it would properly preserve privacy and other civil liberties interests.

For more than 100 years, the ACLU has been our nation's guardian of liberty, working in courts, legislatures, and communities to defend and preserve the individual rights and liberties that the Constitution and the laws of the United States guarantee everyone in this country. The ACLU takes up the toughest civil liberties cases and issues to defend all people from government abuse and overreach. The ACLU is a nationwide organization that fights tirelessly in all 50 states, Puerto Rico, and Washington, D.C., for the principle that every individual's rights must be protected equally under the law, regardless of race, religion, gender, sexual orientation, disability, or national origin.

EFF works to ensure that technology supports freedom, justice, and innovation for all the people of the world. EFF is a non-profit organization with more than 30,000 members. EFF regularly advocates before administrative agencies, courts, and legislatures in support of free speech, data privacy, and other rights at the digital frontier.

We have comments on the following questions posed in the Request for Comment:

2. *Privacy Generally.* Provide comments on what privacy concerns or benefits may arise from mDL transactions, and how DHS should or should not address those concerns and benefits in the REAL ID context. Explain what digital security functions or features are available to protect the privacy of any personally identifiable information submitted in mDL transactions, including the advantages and disadvantages of each security feature.

[1] 86 Fed. Reg. at 20320 (Apr. 19, 2021), https://www.federalregister.gov/documents/2021/04/19/2021-07957/minimum-standards-for-drivers-licenses-and-identification-cards-acceptable-by-federal-agencies-for.

In contemplating regulations for the integration of any kind of digital identity documents into federal processes, the department must recognize that this technology is likely to have ramifications that extend far beyond a simple replacement of plastic IDs by phones, and that radiate far beyond airport gates and other federal agency contexts. Because of the sensitive issues that it raises, we as a nation need to take great care in deciding whether or how we build any such system.

ACLU has published a report on the privacy issues raised by current proposals for a digital driver's license, and attach the full report as a supplement to these comments.[2] We believe that a digital system could enhance user privacy and control if done right—but that it could also become an infrastructure for invading privacy and increasing the leverage and control of government agencies and companies over individuals.

By making it more convenient to show ID and thus easier to ask for it, digital IDs would inevitably make demands for ID more frequent in American life. They may also lead to the routine use of automated or "robot" ID checks carried out not by humans but by machines, causing such demands to proliferate even more. Depending on how a digital ID is designed, it could also allow centralized tracking of all ID checks, and raise other privacy issues. And we would be likely to see demands for driver's license checks become widespread online, which would enormously expand the tracking information such ID checks could create. In the worst case, this would make it nearly impossible to engage in online activities that aren't tied to our verified, real-world identities, thus hampering the ability to engage in constitutionally protected anonymous speech and facilitating privacy-destroying persistent tracking of our activities and associations.

Longer-term, if digital IDs replace physical documents entirely, or if physical-only document holders are placed at a disadvantage, that could have significant implications for equity and fairness in American life. Many people do not have smartphones, including many from our most vulnerable communities. Studies have found that 15 percent of the population does not own a smartphone, including almost 40 percent of people over 65 and 24 percent of people who make less than $30,000 a year.[3] People with disabilities are 20 percent less likely to own a smartphone, and many who are homeless also lack access.[4]

At a bare minimum, DHS should require that any identity system recognized by the federal government:

- **Not allow Verifier access to phones.** Standards and technologies should be designed so that as a practical, real-world matter, Holders (those who carry and present a digital ID)

[2] *See* Am. Civil Liberties Union, *Identity Crisis: What Digital Driver's Licenses Could Mean for Privacy, Equity, and Freedom* (May 17, 2021), https://www.aclu.org/sites/default/files/field_document/20210517-digitallicense.pdf; *see also* Elec. Frontier Found., *Digital Identification Must Be Designed for Privacy and Equity* (Aug. 31, 2020), https://www.eff.org/deeplinks/2020/08/digital-identification-must-be-designed-privacy-and-equity-10.

[3] Pew Rsch. Ctr., *Mobile Technology and Home Broadband 2021* (June 3, 2021), https://www.pewresearch.org/internet/wp-content/uploads/sites/9/2021/06/PI_2021.06.03_Mobile-Broadband_FINAL.pdf.

[4] Pew Rsch. Ctr., *Disabled Americans Are Less Likely to Use Technology* (Apr. 7, 2017), https://www.pewresearch.org/fact-tank/2017/04/07/disabled-americans-are-less-likely-to-use-technology/.

never need to relinquish control of their smartphone to any Verifier (those who are seeking to authenticate the holder). Technology design should be reinforced by policies that prohibit requests by government officials and others to Holders to "voluntarily" hand over devices.

- **Not allow linkable presentations.** Standards and technologies should be designed so that the Issuer of a digital ID (or any of their agents or contractors) cannot know where or to whom a Holder is presenting their ID, and so that Verifiers cannot conspire with each other or with Issuers to track presentations.

- **Provide Holders with granular control over data released.** Standards and technologies should be designed so that Holders have complete control over what data is released from their IDs, including broad flexibility to provide attestations of general categories into which a Holder fits, such as "over age 65" or "a resident of this city."

- **Provide a standardized provisioning process.** The process by which data from DMVs or other Issuers is loaded onto people's devices should be standardized so that anyone can write a compliant digital identity app and Holders will have choices in which app they use.

- **Include transparent source code.** The code for digital identity apps that people install on their phone should be transparent so that members of the public can be assured that it does only what it's supposed to do, and to increase its security.

- **IDs should not "phone home."** Digital identity documents should be designed to be verified offline only, and should be operated entirely offline except when a Holder wants to initiate a specific task related to the ID itself, such as an update or renewal. In particular, this means that Verifiers should not need network access, the Issuer should not be able to assemble a history of uses of any ID, and capabilities like instant remote revocation should not be incorporated into the design.

- **Protect a "right to paper."** People should have a right to obtain and use a paper or other physical identity document instead of or in addition to a digital ID. The use of digital IDs should never become mandatory as a legal or practical matter. Regulations should ensure that all agencies and private actors accept physical IDs on an equal basis and that those who prefer to use physical IDs are not inconvenienced or otherwise disadvantaged.

We believe that it is premature to adopt industry standards at this time as no set of standards has been completed that fully takes advantage of existing privacy-preserving techniques. In recent decades we have seen the emergence of an entire identity community that has been working on the problems of online identity and authorization. Some within the identity community have embraced centralized and/or proprietary systems, while others are animated by a vision of "self-sovereign identity" that is decentralized, open source, privacy-preserving, and empowering of individuals. That movement has created a number of proposed systems, including an open standard created by the World Wide Web Consortium (W3C) called Verifiable Credentials (VCs). The VC concept is still being refined—but so are most efforts in this area, including

efforts at creating mobile driver's licenses by the International Standards Organization (ISO) and the American Association of Motor Vehicle Administrators (AAMVA).

DHS should refuse to recognize IDs presented within centralized identity systems. If a standard digital identity system is to be accepted by the federal government, it must be created in an open, transparent manner, with the input of multiple stakeholders, and based upon the self-sovereign identity concept. Such a system can then be used by federal government agencies to view identity credentials issued by state departments of motor vehicles (DMVs) where doing so makes sense. If standards based on self-sovereign identity are not considered mature enough for adoption, efforts should be directed at rectifying that rather than at adopting other systems that raise privacy, security, and autonomy risks.

Current industry standards have also been developed through a process that has not been open to the broad range of stakeholders. An identity system is a not an obscure industrial standard, but a highly sensitive matter with significant implications for individual privacy, equity, and the relationship between citizens and their government. We live in a democracy, yet crucial decisions about our new potential identity infrastructure are being made by a working group within the ISO whose American members seem to consist primarily of representatives of corporations, AAMVA, and government agencies. The ISO is a private entity and hardly exhibits the transparency that an organization whose activities have such important public implications ought to have. The ISO will not even disclose the working group's membership list. It's practically impossible for any interested party to join this secret committee, their deliberations are not open to the public, and their drafts and other work products are treated like classified documents. There are also representatives of authoritarian countries in the ISO who would like to surveil ID holders instead of protect their privacy.

This lack of openness and democracy shows—for example in the standards' failure to make unlinkable presentations a central feature.

AAMVA, like the ISO, is a private entity, not subject to the checks and balances that apply to government agencies like DHS. AAMVA may argue, for example, that the Freedom of Information Act does not apply to it. While AAMVA is playing a role much like a government agency in pushing digital driver's licenses, it may evade the transparency obligations that apply to civilian government agencies. Many of its key documents are not available to the public, and it claims copyright in the materials that it produces. In the past, it has removed controversial documents from its site and sent copyright takedown notices to critics who are monitoring its activities.

All this is in stark contrast to W3C, the developer of the "Verifiable Credentials" standards, where the work is done through an open public process, participation is far more open, and meeting notes, recordings, and materials are accessible to all.

Finally, we are concerned about the proposal's layering of REAL ID with mDL. REAL ID has many privacy problems,[5] which should not be carried over into mDLs. Moreover, if a person had an mDL issued by a state DMV, that would address forgery and cloning concerns, without the need for REAL ID and its privacy problems.

5. Industry Standard ISO/IEC 23220-3: Communication Interface Between DMV and mDL Device. DHS understands that forthcoming international industry standard ISO/IEC 23220-3 may specify digital security mechanisms and protocols with respect to the communication interface between a DMV and a mobile device, specifically concerning provisioning methods, data storage, and related actions. Although DHS may seek to adopt certain requirements anticipated to appear in this standard, the Department understands that this standard may not be finalized for several years.

a. Explain whether commenters believe the current drafts of standard ISO/IEC 23220-3 are mature enough to support secure and widespread deployment of mDLs.

There are no publicly disclosed drafts of ISO/IEC 23220-3. This makes it impossible for the general public to provide informed comment on this question. If the only people able to evaluate a standard in development are the undisclosed parties involved in an opaque process that generates the standard itself, it is inappropriate to use comments from only those implementers as a basis for decisions about public policy.

6. Provisioning. DHS understands that provisioning may be conducted in-person, remotely, or via other methods.

a. Explain the security and privacy risks, from the perspective of any stakeholder, presented by in-person, remote, or other provisioning methods.

It is important that the provisioning process be based on open standards in order to protect the security and privacy of those who install digital ID apps. An open standard would allow anybody to create an app that would interface with a DMV simply by complying with those standards. This would allow a variety of developers—including public-minded/nonprofit developers—to create competing ID apps, giving consumers a choice in which app to use.

It's important that consumers be able to use apps that have transparent source code so that experts (or any member of the public so inclined) can scrutinize them to confirm their operation and security. These are apps that will be carrying out an essential public function, so people need to be able to receive assurance that the apps a) only do what they are supposed to do and b) are as secure as their designers claim.

Many or all of the private companies that make the apps on behalf of DMVs may want to keep their code proprietary. That would mean that ID holders are running what is essentially secret government code on their phones and reduced to merely trusting in its operation and security.

[5] *See, e.g.*, Am. Civil Liberties Union, *Real ID*, https://www.aclu.org/issues/privacy-technology/national-id/real-id (last visited July 29, 2021); Elec. Frontier Found., *Real ID: Threatening Your Privacy Through an Unfunded Government Mandate*, https://www.eff.org/issues/real-id (last visited July 29, 2021).

That is not acceptable—and even less so if people are legally or practically required to use mDLs.

If policymakers fail to require that all mDL apps reveal their source code, open standards for the provisioning process would also help give consumers the ability to choose an open-source application they can trust.

8. Data Freshness. Provide comments regarding whether and to what extent security risks concerning data validity and freshness can be mitigated by defining the frequency by which mDL Data should synchronize with its DMV database.

a. Provide comments regarding what data synchronization periods commenters believe are appropriate for mDL transactions. Explain the advantages and disadvantages of a longer or shorter periods.

While there may be scenarios where outdated information in a digital identity certificate is important, the information that federal agencies such as the TSA most commonly want to confirm rarely changes, such as date of birth (never) and name (rarely more than once or twice in a lifetime). Where digital driver's licenses are used to confirm ID, such as at TSA checkpoints, it does not matter whether a Holder's driving privileges have been revoked.

Balanced against these weak benefits, the privacy compromises that would need to be made to ensure the "freshness" of ID data would be unacceptable. Designing digital IDs that can be remotely updated would require those IDs to "phone home" to their Issuers (such as DMVs) on a regular basis. This would expose the Holder's IP address, from which their location can sometimes be inferred—both potentially sensitive pieces of information. Given that physical licenses are only updated every 4-12 years, depending on the issuing state, there is no reason to compromise the privacy of digital licenses in order to allow for greater freshness.[6] Insisting upon doing so would strongly suggest that DHS intends for digital driver's licenses to eventually become mandatory instead of remaining an optional alternative to physical licenses—something that in our view would cause enormous problems and which our nation should not allow.

11. Offline and Online Data Transfer Modes. DHS understands that mDL Data may be transferred to a Federal agency via offline and online modes.

a. Explain the security and privacy risks, from the perspective of any stakeholder, presented by both offline and online data transfer modes.

b. Provide comments on the security protocols that would be required to mitigate security and privacy risks presented by both offline and online data transfer modes.

A crucial characteristic of any acceptable digital identity system is that it must prevent identity Issuers and any other party from automatically tracking identity presentations. The "online data transfer mode" discussed in this Request for Comment, allowing for communication between

[6] Ins. Inst. for Highway Safety, *License Renewal Procedures by State* (July 2021), https://www.iihs.org/topics/older-drivers/license-renewal-laws-table.

DMVs and federal agencies when those agencies are verifying IDs, and included in the draft ISO/IEC 18013-5 standard, is incompatible with a system that provides robust technological protection of unlinkable presentations.

When someone visually inspects a plastic driver's license, no record of that inspection is automatically generated, retained, or shared with the DMV. With a shift from plastic to digital identities, such tracking becomes possible. It is especially important that unlinkable presentations be built into a digital identity system given that such a system may expand to cover more and more uses. Currently, mDLs are being framed narrowly as replacements for physical ID cards, to be deployed in TSA checkpoints, traffic stops, alcohol purchases, and the like. But, once entrenched in that role, digital IDs are likely to expand into a far broader role in proving identity than driver's licenses play today. Indeed, many of those involved in the development of mDLs envision just such an expansion. For example, the global ISO working group is planning a second phase of standards-writing to enable the presentation of mDLs over the Internet.[7] Also, Google and Apple's operating system work in this area is largely focused on building the capacity for online presentations. Likewise, AAMVA declares that "new use cases brought about by the nature of an mDL can be expected. Online use is one example."[8]

We may also see an expansion of the data that is held in these digital IDs. As one state official put it, "you can use it for hunting and fishing licenses, weapons' permits, tax returns—all sorts of things."[9]

If a digital identity system is to be adopted, standards and technologies must be designed so that the Issuer (or any of their agents or contractors) cannot know where or to whom a Holder is presenting their ID, and to minimize the ability of Verifiers to conspire with each other or with Issuers to compile records of presentations. Policy protections for non-linkability of presentations alone are not sufficient, especially given the vast amount of personal information that a digital identity system could grow to include.

12. Unattended Online mDL Verification. Provide comments on what capabilities or technologies are available to enable unattended online mDL verification by Federal agencies. Explain the possible advantages and disadvantages of each approach.

a. Explain the security and privacy risks, from the perspective of any stakeholder, presented by unattended online mDL verification.

One significant risk of unattended ID verification is that the TSA or other federal agencies will not devote sufficient resources to make sure that those who present physical IDs are not subject

[7] Secure Tech. Alliance, *The Mobile Driver's License (mDL) and Ecosystem* (2020), https://www.securetechalliance.org/wp-content/uploads/Mobile-Drivers-License-WP-FINAL-Update-March-2020-4.pdf.

[8] Am. Assoc. of Motor Veh. Administrators, *Mobile Driver's License Functional Needs White Paper* (Jan. 2019), https://www.aamva.org/FunctionalNeedsWhitepaper-9/.

[9] Jenni Bergal, *As States Push for Digital Drivers Licenses, Critics Cite Privacy Concerns*, Huff. Post (Nov. 20, 2018), https://www.huffpost.com/entry/could-plastic-drivers-licenses-become-a-thing-of-the_b_5bf41780e4b09851702fe10e.

to longer lines or other inconveniences, helping turn digital IDs into de facto mandatory credentials.

14. Considerations for mDL Devices Other than Smartphones. Provide comments on whether provisioning an mDL on, or accessing an mDL from, a device other than a smartphone (e.g., a smartwatch accessing mDL Data from a smartphone paired to it, or a mobile device authorized to access mDL Data stored remotely), poses security or privacy considerations different than provisioning an mDL on, or accessing an mDL from, a smartphone. Explain such security or privacy considerations and how they can be mitigated.

We believe that physical licenses must always remain an equal alternative to digital IDs. Digital IDs that are legally or practically mandatory would:

- Further marginalize those without access to the relevant technology, whether that is a smartphone or other mDL device. Affordable quality Internet connectivity may also pose a challenge to using an mDL app (on a smartphone or otherwise) if it requires online provisioning and frequent updates.

- Set a terrible precedent for the forced adoption of technology, whether that is an installation of apps on people's phones, wristbands or other trackers. Personal digital devices should be under the control of, and serve to empower, their owners. People should not become prisoners of their own phones as various government agencies use compulsory app installation rules to turn them into surveillance and enforcement devices for all kinds of legal and administrative rules. Our IDs, whether on a smartphone or not, should not become the functional equivalent of ankle bracelets — mandatory devices that must be carried at all times and which serve as an instantly and remotely controllable government lever over citizens.

- Open up new possibilities of abuse. A poorly designed digital ID could allow for abusive revocation, monitoring, and lack of due process by capricious officials or politicized law enforcement agencies, which we have seen too often in our history.

- Leave people susceptible to technology failures. Digital devices (including smartphones) fail, sometimes at random times and for no apparent reason. Entries in centralized databases can get corrupted, hacked, or inexplicably deleted. A purely digital system is not as robust against such failures as a system based on physical documents.

15. Obstacles to mDL Acceptance. Describe any obstacles to public or industry acceptance of mDLs that DHS should consider in developing its regulatory requirements. Provide comments on recommendations DHS should consider addressing such obstacles, including how to educate the public about security and privacy aspects of digital identity and mDLs.

In a country like ours with understandably high levels of suspicion of government, any system of digital identity documents — already a fraught undertaking due to its potential overuse — will

need to include the strongest possible privacy protections to have any chance of being embraced by a wide spectrum of Americans.

Thank you for considering our views. Please reach out to Jay Stanley (JStanley@aclu.org) and Kathleen Ruane (KRuane@aclu.org) with any further questions.

Sincerely,

American Civil Liberties Union
Electronic Frontier Foundation (EFF)
Electronic Privacy Information Center (EPIC)